

UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

2018 APR 24 PM 2:00

UNITED STATES OF AMERICA,

v.

DONALD HAMMALIAN, JR.,

Defendant.

CLERK
BY 
DEPUTY CLERK

Case No. 2:17-cr-00070

**OPINION AND ORDER DENYING
DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AND STATEMENTS**
(Doc. 38)

Defendant Donald Hammalian, Jr. is charged with two counts of possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). Pending before the court is Defendant's motion to suppress information obtained from service providers Google and Comcast without a warrant in violation of the Fourth Amendment, as well as evidence and statements subsequently obtained from him through the use of the information provided by Google and Comcast as fruits of an illegal search. (Doc. 38.)

Defendant filed his motion to suppress on December 22, 2017. The government filed its opposition to the motion on February 2, 2018. On February 21, 2018, the court set the matter for a hearing to be held on April 20, 2018, however, on April 18, 2018, the parties agreed that the court should decide Defendant's motion on the pleadings without an evidentiary hearing or oral argument.

Defendant is represented by Assistant Federal Public Defender Steven L. Barth. Assistant United States Attorney Barbara A. Masterson represents the government.

I. Factual Background.

In August 2016, the New York City Police Department ("NYPD") arrested an individual for child pornography offenses. The arrested individual provided the officers written consent and the passwords needed in order to search email accounts he had admitted to using for the purpose of trading child pornography. During this search, law

enforcement found an email dated July 22, 2016 from the email address theandreahenderson5@gmail.com which contained links to websites that contained images of child pornography.

NYPD forwarded this email address to Department of Homeland Security investigators, who issued a summons to Google on August 26, 2016. The summons sought:

[A]ll records regarding the identity of the following customer to include, but not limited to, registrant name, address, associated email addresses, all [media access control (“MAC”)] addresses, telephone number, status of account, available [internet protocol (“IP”)] history, length of service, and date account was opened concerning the account using the email address: theandreahenderson5@gmail.com.

(Doc. 38 at 2.) The summons further explained that it was issued pursuant to 19 U.S.C. § 1509 and that Google was “not to disclose the existence of this summons for an indefinite period of time.” *Id.* (internal quotation marks omitted).

Google responded to the summons by providing “subscriber information, including the name [associated with the account], email address, services used, creation date, login information, account [identification] number and IP addresses.” (Doc. 42 at 2.) Once the investigators determined that the IP addresses provided were controlled by Comcast, they sent a summons to Comcast on September 21, 2016 seeking:

[A]ll records regarding the identity of the following customer to include, but not limited to, registrant name, address, email addresses, all MAC addresses, telephone number, status of account, available IP history, length of service, and date [the] account was opened concerning the account using [two specifically identified IP addresses] on [July 1 and 10, 2016 at specific times].

(Doc. 38 at 2.) This summons also explained that it was issued pursuant to 19 U.S.C. § 1509 and required Comcast “not to disclose the existence of this summons for an indefinite period of time.” *Id.* at 3 (internal quotation marks omitted).

Comcast's response identified the account subscriber¹ and "detailed the service[s] [used] and billing addresses, telephone number, type of service, account number, date [the] service began, account status, IP history, MAC address, and the email user [identification]." (Doc. 42 at 2.)

Based on the foregoing information, on November 9, 2016, investigators obtained a search warrant for Defendant's residence located at 21 Garden Lane, Bennington, Vermont. They executed the warrant on November 10, 2016. On January 10, 2017, the agents obtained a second search warrant to search Defendant's Bennington residence after they reviewed video of the first search warrant's execution taken through a surveillance system set up in Defendant's residence. The video appeared to show Defendant hiding a digital device while the agents were outside his residence knocking and announcing their presence. A forensic examination of digital media found during the execution of the second search warrant revealed the alleged presence of child pornography.

II. Conclusions of Law and Analysis.

Defendant argues that the investigators violated the Fourth Amendment in obtaining records from Google and Comcast without a warrant, contending that he had a reasonable expectation of privacy in the account information provided to the government. The government responds that no Fourth Amendment violation occurred because Defendant does not have a reasonable expectation of privacy in business records maintained by a third party.

The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. "[A] Fourth Amendment search occurs when the government violates a subjective

¹ The government asserts that Comcast's response identified Defendant as the account subscriber.

expectation of privacy that society recognizes as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

“The Supreme Court has long held that a ‘person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,’ including phone numbers dialed in making a telephone call and captured by a pen register.” *United States v. Ulbricht*, 858 F.3d 71, 96 (2017) (quoting *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979)). “[P]hone users typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.” *Id.* (internal quotation marks omitted). “Similarly, e-mail and Internet users . . . [also] rely on third-party equipment in order to engage in communication.” *Id.* (citing *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)) (internal quotation marks omitted). Internet users therefore “should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.” *Id.* (internal quotation marks omitted). “IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers.” *Id.* (internal quotation marks omitted).²

In *Ulbricht*, the Second Circuit affirmed the denial of the defendant’s motion to suppress information obtained from “the pen/trap orders that the government used to monitor IP address traffic to and from his home router[.]” *Id.* at 95. The court found that the “recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in *Smith [v. Maryland]*.” *Id.* at 97. The Second Circuit thus “join[ed] the other

² While *Ulbricht* noted that “some aspects of modern technology, which entrust great quantities of significant personal information to third party vendors,” have led to a “call for a re-evaluation of the third-party disclosure doctrine established by *Smith*[.]” the Second Circuit “remain[ed] bound, however, by [the *Smith*] rule until and unless it is overruled by the Supreme Court.” *United States v. Ulbricht*, 858 F.3d 71, 96-97 (2017).

circuits that have . . . [held] that collecting IP address information devoid of content is constitutionally indistinguishable from the use of a pen register.” *Id.* at 97.³ In doing so, the *Ulbricht* court observed that:

The substitution of electronic methods of communication for telephone calls does not alone create a reasonable expectation of privacy in the identities of devices with whom one communicates. Nor does it raise novel issues distinct from those long since resolved in the context of telephone communication, with which society has lived for the nearly forty years since *Smith* was decided. Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information.

Id.

In this case, the investigators obtained subscriber information from internet providers Google and Comcast, including the account holder’s name, billing and email addresses, telephone number, services used, account creation date and status, login information, account identification number, IP addresses and history, and MAC addresses. Defendant voluntarily turned over this information to these third-party internet providers, who did not disclose the content of any communications to the government. As a result, Defendant had no reasonable expectation of privacy in the information obtained by the investigators under *Ulbricht*.

³ See *United States v. Carpenter*, 819 F.3d 880, 887 (6th Cir. 2016) (“[C]ourts have not (yet, at least) extended [Fourth Amendment] protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses.”); *United States v. Graham*, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (noting that “third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection”); *United States v. Wheelock*, 772 F.3d 825, 828 (8th Cir. 2014) (holding that the defendant “cannot claim a reasonable expectation of privacy in [the] government’s acquisition of his subscriber information, including his IP address and name, from third-party service providers.”) (internal quotation marks omitted); *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) (holding that there is no expectation of privacy in “subscriber information provided to an internet provider[,]” such as an IP address) (internal quotation marks omitted); see also *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (holding that “computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator.”).

Defendant maintains that *Smith* and *Ulbricht* are distinguishable because the investigators sought “a much wider range of information” and obtained information “beyond IP addresses[,]” including “logs that tend to reveal location information[.]” (Doc. 38 at 8 n.3.) He argues that a five-justice majority in *United States v. Jones*, 565 U.S. 400 (2012) found that “longer term GPS monitoring” constituted a search under the Fourth Amendment. *Id.* at 430 (Alito, J., concurring); *see also id.* at 415 (Sotomayor, J., concurring).

The majority opinion in *Jones*, however, “did not address the third-party disclosure doctrine, let alone purport to desert or limit it.” *United States v. Wheelock*, 772 F.3d 825, 829 (8th Cir. 2014). “Of the separately concurring justices, only Justice Sotomayor voiced any dissatisfaction with the doctrine, and even then, she did not outright advocate its abandonment.” *Id.* Bound by the third-party disclosure doctrine articulated in *Smith*, “[f]ederal courts have uniformly held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation because it is voluntarily conveyed to third parties.” *United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) (internal quotation marks omitted); *see also United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (“Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment’s privacy expectation.”). Courts have distinguished cases such as *Jones*, which involve the government’s use of surveillance technology to “track an individual’s” location, from the issue of “whether the government invades an individual’s reasonable expectation of privacy when it obtains, from a third party, the third party’s records, which [subsequently] permit the government to deduce location information.” *United States v. Graham*, 824 F.3d 421, 426 (4th Cir. 2016). In that case, “the third-party doctrine . . . provide[s] the answer.” *Id.* at 427.

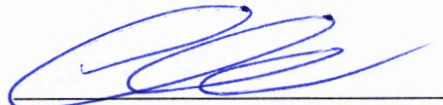
Defendant further contends that the third-party disclosure doctrine is not “a hard and fast rule and is instead simply one factor in the overall reasonable expectation of privacy analysis.” (Doc. 38 at 8.) The third-party disclosure doctrine is nevertheless “dispositive” to the extent that Defendant “cannot claim a reasonable expectation of

privacy in the government's acquisition of his subscriber information, including his IP address and name from third-party providers." *Wheelock*, 772 F.3d at 828-29 (internal quotation marks omitted).⁴

CONCLUSION

For the foregoing reasons, Defendant's motion to suppress evidence and statements obtained in violation of the Fourth Amendment (Doc. 38) is DENIED. SO ORDERED.

Dated at Burlington, in the District of Vermont, this 24th day of April, 2018.



Christina Reiss, District Judge
United States District Court

⁴ The court need not reach the issue of whether the good faith exception to the Fourth Amendment's exclusionary rule applies.